Security zSecure Service Stream Enhancement for
PCI-DSS support
Version 2.1.0

Documentation updates for User Reference Manual for ACF2

Security zSecure Service Stream Enhancement for PCI-DSS support
Version 2.1.0

Documentation updates for User Reference Manual for ACF2

IBM

Chapter 1. User Reference Manual: System Audit Guide

This chapter provides the updates to the System Audit Guide chapter in the User Reference Manual as a result of the IBM Security zSecure V2.1 Service Stream Enhancement for PCI-DSS support:

- “Preparation”
- “Reporting”
- “Rule examples” on page 2
- “Checking that permissions are limited to the compliant population” on page 2

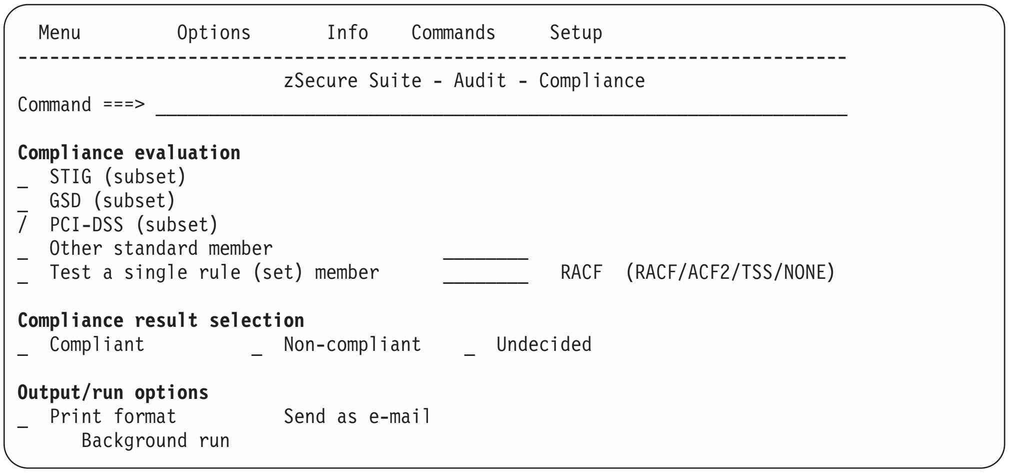
Preparation

The following members for the CKACUST data set were added to the table:

Member	User group
CLASSIFY	Member for PCI-DSS SIMULATE SENSITIVE statements
PCIAUTH	Users allowed to access resources containing payment card Sensitive Authentication data
PCIPAN	Users allowed to access resources containing payment card Primary Account Numbers

Reporting

The Audit - Compliance panel and subsequent descriptions changed as follows:



```
  Menu         Options       Info    Commands     Setup
------------------------------------------------------------------------------
                         zSecure Suite - Audit - Compliance
Command ===> _________________________________________________________________

Compliance evaluation
_  STIG (subset)
_  GSD (subset)
/  PCI-DSS (subset)
_  Other standard member                 ________
_  Test a single rule (set) member       ________   RACF  (RACF/ACF2/TSS/NONE)

Compliance result selection
_  Compliant          _  Non-compliant    _  Undecided

Output/run options
_  Print format          Send as e-mail
      Background run
```

The **STIG**, **GSD**, and **PCI-DSS** selections refer to predefined subsets for these standards:

STIG Security Technical Implementation Guide published by the US Defence Information Systems Agency (DISA-STIG)

GSD IBM standard often employed in outsourcing (GSD331)

PCI-DSS
Payment Card Industry Data Security Standard

Rule examples

The following naming conventions were added to the list:

- CKAPB* members are RACF PCI-DSS version 2.0 rules.
- C2APB* members are ACF2 PCI-DSS version 2.0 rules.

Checking that permissions are limited to the compliant population

The introduction changed as follows:

CARLa DEFTYPEs are used to look up IDs in the CKACUST members that specify the compliant populations. For the STIG, standard DEFTYPEs of the form TYPE=POPULATE_STIG_*member* are used. For PCI-DSS, standard DEFTYPEs of the form TYPE=POPULATE_PCI_*member* are used.

Chapter 2. User Reference Manual: SMF and HTTP reporting (Events menu)

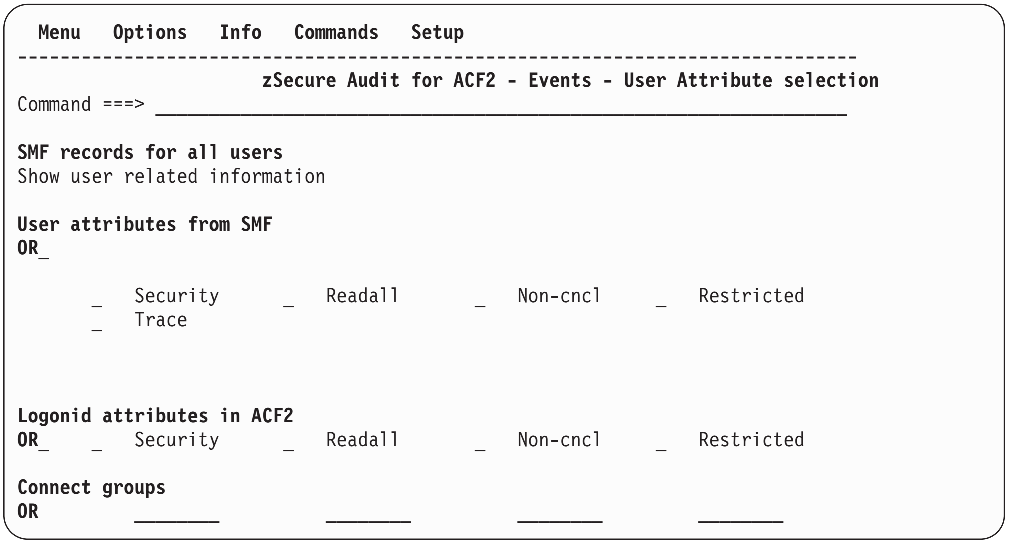
This chapter provides the updates to the SMF and HTTP reporting (Events menu) chapter in the User Reference Manual as a result of the IBM Security zSecure V2.1 Service Stream Enhancement for PCI-DSS support:

- “User attributes”
- “Advanced selection criteria: (Further) IP selection”
- “DATASET - Data set events from SMF” on page 4

Note: Links to sections in the User Reference Manual that are not included in this document do not work.

User attributes

The Events - User Attribute selection panel was added:



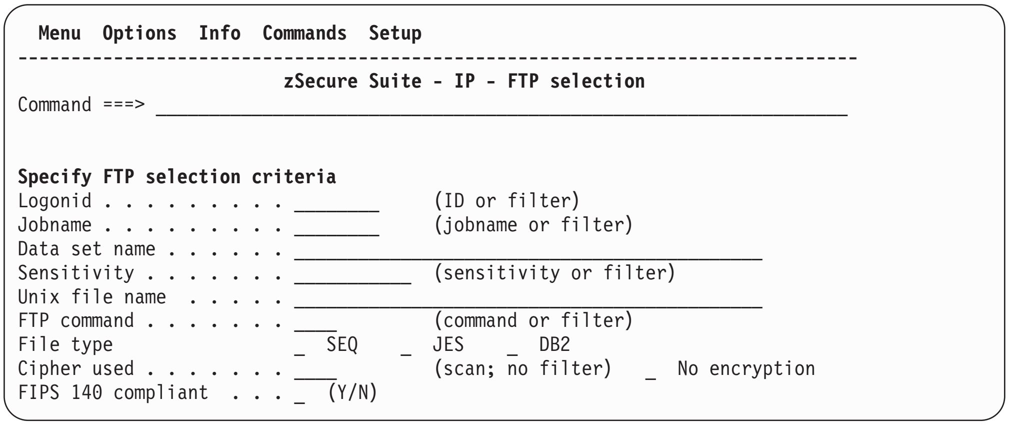
```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                       zSecure Audit for ACF2 - Events - User Attribute selection
Command ===> __________________________________________________________________

SMF records for all users
Show user related information

User attributes from SMF
OR_

       _   Security      _   Readall       _   Non-cncl     _   Restricted
       _   Trace



Logonid attributes in ACF2
OR_    _   Security      _   Readall       _   Non-cncl     _   Restricted

Connect groups
OR         ________      ________          ________         ________
```

Figure 1. Events User Attribute Selection panel

Advanced selection criteria: (Further) IP selection

The FTP Selection panel was added:

When you select **FTP**, the following selection panel is displayed.



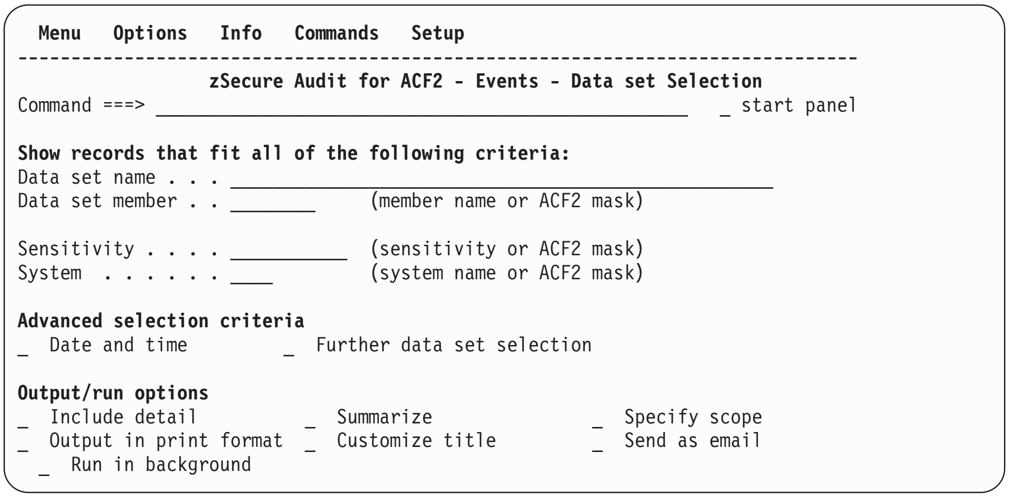
```
  Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                         zSecure Suite - IP - FTP selection
Command ===> _________________________________________________________________


Specify FTP selection criteria
Logonid . . . . . . . . ________     (ID or filter)
Jobname . . . . . . . . ________     (jobname or filter)
Data set name . . . . . ____________________________________________
Sensitivity . . . . . . ___________  (sensitivity or filter)
Unix file name  . . . . ____________________________________________
FTP command . . . . . . ____         (command or filter)
File type               _  SEQ    _  JES    _  DB2
Cipher used . . . . . . ____         (scan; no filter)   _  No encryption
FIPS 140 compliant  . . . _  (Y/N)
```

Figure 2. Events - FTP Selection panel

For detailed field information, press **PF1** on the selection panel or any field to open the help.

DATASET - Data set events from SMF

The Events Data set Selection panel was changed as follows:



```
  Menu   Options   Info   Commands   Setup
--------------------------------------------------------------------------------
                  zSecure Audit for ACF2 - Events - Data set Selection
Command ===> __________________________________________________   _ start panel

Show records that fit all of the following criteria:
Data set name . . . ___________________________________________________
Data set member . . ________     (member name or ACF2 mask)

Sensitivity . . . . ___________  (sensitivity or ACF2 mask)
System  . . . . . . ____         (system name or ACF2 mask)

Advanced selection criteria
_  Date and time         _  Further data set selection

Output/run options
_  Include detail          _  Summarize                _  Specify scope
_  Output in print format  _  Customize title          _  Send as email
  _  Run in background
```

Figure 3. Events Data set Selection panel

Chapter 3. User Reference Manual: calling zSecure

As a result of the IBM Security zSecure V2.1 Service Stream Enhancement for PCI-DSS support, the section Naming conventions for PCI-DSS SCKRCARL members was now added.

Naming conventions for PCI-DSS SCKRCARL members

PCI-DSS consists of twelve security requirements. Each requirement further consists of sub-requirements which are uniquely identified by requirement numbers. These requirement numbers are used in the naming of PCI-DSS SCKRCARL members for traceability. In general, PCI requirement X.Y.Z can be found in C%APBXYZ member. Alphabetical characters are used to count beyond 9. So, for example:

- RACF PCI-DSS requirement 8.5.9 can be found in the SCKRCARL member CKAPB859.
- ACF2 PCI-DSS requirement 8.5.10 can be found in the SCKRCARL member C2APB85A.

Chapter 4. User Reference Manual: SELECT/LIST Fields

This chapter provides the updates to the SELECT/LIST Fields chapter in the User Reference Manual as a result of the IBM Security zSecure V2.1 Service Stream Enhancement for PCI-DSS support:

- IP_TELNET_REGION: TelnetGlobal block settings: the field `TNSACONFIG_SNMP_ENABLED` was removed from the documentation.
- "SMF: SMF records": several field descriptions were added or changed.
- "Record types vs. field names" on page 12: Table 1 on page 12 was changed to reflect the changes in `NEWLIST TYPE=SMF`.

Note: Links to sections in the User Reference Manual that are not included in this document do not work.

SMF: SMF records

The following fields were added or changed:

APPLDATA

The socket application data as it has been set by the application by an SIOCSAPPLDATA ioctl() call to further identify the purpose of the port. This field is 40 characters wide. It is present for TCP socket close SMF records (119-2).

BYTES_IN

This is the number of bytes transferred into the local system, for instance by FTP, TN3270, or SMTP. It is present for:

- SMF 118 subtypes for FTP (71, 73, 74), TELNET (20, 21), and API (1, 2)
- SMF 119 subtypes for TCP socket close (2), FTP client transfer completion (3), UDP socket close(10), Telnet server connection termination (21), Telnet client connection termination(23), CS-SMTP connection (49), and FTP server transfer completion (70)

BYTES_OUT

This is the number of bytes transferred from the local system, for instance by FTP, TN3270, or SMTP. It is present for:

- SMF 118 subtypes for FTP (71, 73, 74), TELNET (20, 21), and API (1, 2)
- SMF 119 subtypes for TCP socket close (2), FTP client transfer completion (3), UDP socket close(10), Telnet server connection termination (21), Telnet client connection termination(23), CS-SMTP connection (49), and FTP server transfer completion (70)

CIPHER

This field represents the negotiated cipher. This is a 4 character cipher number, a 2 character cipher number (pre-z/OS 2.1), or missing (pre-z/OS 1.8 SMF). It is present for SMF 119 record subtypes 2 (TCP socket closed), 3 (FTP client transfer complete), 70 (FTP server transfer complete), and 72 (FTP server logon failure). For FTP record types 19-2 and 119-70, the field `FTP_CIPHERSUITE` might be more readily understandable.

CSSMTP_CN_FIPS140

Flag field indicating whether the connection is compliant with FIPS 140. FIPS140 is an alias for this field name. See FIPS140 for a description.

DSTIP

Destination IP address. This field is found in z/OS® Firewall Technologies records, SMF record type 109, SMF record type 118 (IPv4), SMF record type 119 (IPv6) and in EIM auditing records (type 83 subtype 2) where it is extracted from the EIM domain name. In record types 109, 118 and 119 it always is an IP address, in the EIM records it will mostly be a hostname.

Note that for both FTP server (119-70) and client (119-3) SMF records, DSTIP is on the local z/OS system writing the SMF record, and SRCIP is the possibly remote communication partner.

FIPS140

This flag field indicates whether the connection is compliant with FIPS 140. It is set for SMF 119 subtypes 2, 3, 49, 70, 72, 73, 74, 75, and 76 if the transfer was done with FIPS 140 compliant encryption. This field is an alias name for CSSMTP_CN_FIPS140.

FTP_CIPHERSUITE

This repeated field shows the names of cipher algorithms that can be used during the TLS handshake, as specified on the CIPHERSUITE statement. The name can be interpreted as follows: SSL_*cipher_cipher-hash*[_EX]

The order of the algorithms denotes the priority order. The client and server specify the list of encryption types that they support. The client and server negotiate which of the available ciphers is used for the data encryption by specifying the desired ciphers in order of preference. The actual cipher used is the best match between what the server supports and what the client requests. If the server does not support any of the ciphers that the client requests, the TLS handshake fails and the connection is closed. The CIPHERSUITE statements are used by the FTP server when the EXTENSIONS statement is coded with the AUTH_TLS value. The CIPHERSUITE statements are used by the FTP client when the SECURE_MECHANISM TLS statement is coded or when the FTP client is started with either the -a TLS or the -r TLS start parameter.

For FTP server (119-70) and client (119-3) SMF records, this field returns the 20 character cipher specification field from the SMF record.

FTP_FILETYPE

Reflects the FILETYPE statement used to specify the method of operation for FTP. It is present for SMF 118 (71, 73, 74) and SMF 119. For FTP server (119-70) and client (119-3) SMF records, this field returns the file type of the actual transfer.

JES Remote job submission.

SEQ MVS data sets or z/OS UNIX files. SEQ is the method of operation supported by all FTP platforms. This is the default.

SQL SQL query function. SQL method affects the RETR command at the server and the PUT subcommand at the client.

FTP_SECURE_CTRL_CONN

Reflects the SECURE_CTRLCONN statement used to indicate the security level for a control connection. This statement applies only to Kerberos. When using TLS, the control connection must be enciphered and this setting has no effect on the TLS behavior. EXTENSIONS AUTH_GSSAPI must be set for this statement to be used by the FTP server. The possible values are:

CLEAR
Specifies that the client decides whether data is transferred raw, integrity protected only, or both integrity and privacy protected.

PRIVATE
Specifies that the server requires data to be transferred using both integrity and privacy protection. Clients attempting to send raw data or data integrity protect only are rejected.

SAFE Specifies that the server requires data to be transferred using integrity protection only, or using both integrity and privacy protection. Clients attempting to send raw data are rejected.

For FTP server (119-70) and client (119-3) SMF records, this field returns the Kerberos security setting for the control connection used during the actual transfer.

FTP_SECURE_DATA_CONN
This field reflects the SECURE_DATACONN statement to indicate the level of security used on data connections and it applies to both TLS and Kerberos. If the FTP server uses the secure port (see field FTP_TLS_PORT), the server behaves as if the value on this statement is PRIVATE.

NEVER
Indicates that the server requires data to be transferred raw with no cipher algorithm applied to the data. Clients attempting to use ciphers are rejected.

CLEAR
Indicates the client decides whether data is transferred raw or enciphered. For TLS, the client decides whether data is enciphered or not. If it indicates it should be enciphered, the cipher algorithm is chosen using TLS protocols. For Kerberos, the client can specify whether data is transferred raw, integrity protected only, or both integrity and privacy protected.

PRIVATE
Indicates the server requires data to be transferred enciphered. Clients attempting to send raw data are rejected. For TLS, the cipher algorithm is chosen using TLS protocols. For Kerberos, the data must be transferred using both integrity and privacy protection. Clients attempting to send data that is only integrity protected are rejected.

SAFE For TLS, specifying this option is identical to the PRIVATE specification. For Kerberos, the data must be transferred using both integrity and privacy protected. Clients attempting to send data that is only integrity protected are rejected.

For FTP server (119-70) and client (119-3) SMF records, this field returns the Kerberos security setting for the data connection used during the actual transfer.

JOBNAME

Job or session name. This field is found in all job records.

The JOBNAME field is omitted if it is present in the record but only contains hex null characters. This most often occurs with TSO user logons (RACF® processing records with EVENT=1) and with accesses during the logon process of a TSO user.

If the optional correlation header section is present in the SMF record and the field contains nonblank, nonnull information, this field is also available in the SMF record types: 100, 101, 102, and 110. It can also be found in all SMF 119 record subtypes if non-blank and not null.

PACKETS_IN

This is the number of UDP datagrams or TCP packet sections transferred to the local system. It is present for SMF 119 subtypes 2 (TCP socket close), and 10 (UDP socket close).

PACKETS_OUT

This is the number of UDP datagrams or TCP packet sections transferred from the local system. It is present for SMF 119 subtypes 2 (TCP socket close), and 10 (UDP socket close).

PRIV_USER_GROUPS

This repeating field returns privileged group names for the user ID. These are the connect groups for `USER` that are also present in a `SIMULATE PRIV_USER_GROUPS` command. The field returns no more than 4,000 group names. If the number of privileged groups exceeds 4,000, they will be the alphabetically first 4,000 privileged groups. In principle, the field can be filled in for any SMF record type that returns a value in the field `USER` that exists in the security database of the system.

R_MGMT_CMD

The R_MGMT_CMD field identifies the application-specific command that was being performed during the event that generated this record. This field can be found in security audit event records from IBM® Websphere Application Server (SMF record type 83, subtype 5). The value is taken from relocate section 154 (`mgmtCmd`).

It is present for SMF 118 (71,72,73,74) and SMF 119. For both FTP server (119-70) and client (119-3) SMF records, this field returns the 4 character RFC-compliant FTP command.

R_USER

The `R_USER` field contains the userid used by the product or component for purposes of the authentication or authorization request that generated this record. This field is found in Security Key Lifecycle Manager audit records (SMF record type 83, subtype 6). The value is taken from the relocate section 150 (`user=[name=`*`name`*`]`) of the record.

This field also applies to security audit records from IBM Websphere Application Server (SMF record 83, subtype 5). In these records, the value is taken from relocate section 113 (`accApplUser`) of the record.

For the FTP client (119-3) SMF record, this field returns the remote user identification used to login to the remote FTP server.

For the TCP socket close (119-2) SMF record, this field returns the AT-TLS partner user ID that is part of the partner digital certificate.

SENSTYPE, SENSITIVITY

Sensitivity for the object. This field is 11 wide. It can be filled in for any record type that fills in DSNAME. The data set name and volume serial must match the ones shown in `TYPE=SENSDSN` and the CKFREEZE must belong with the SMF in time (that is, it must be allocated with the same VERSION). See table SENSDSN: Sensitivity types and descriptions for a list of built-in sensitivities. A CKFREEZE file with data set information must be present for this field to be properly filled in, like for `TYPE=SENSDSN`.

SRCIP

Source IP address. This field is found in the following record types:

- z/OS Firewall Technologies records
- SMF record type 109, SMF record type 118 (IPv4)
- SMF record type 119 (IPv6)
- SMF record type 102 subtype/IFCid 269 and 319
- SMF record type 110 subtype 1 (CICS® performance monitoring record)
- SMF record type 83 subtype 5 (audit records from IBM Websphere Application Server)
- SMF record type 42 subtype 26 (NFS audit statistics)

For Websphere Application Server audit records, the value is taken from relocate section 106 (`sessRemAddr`) of the record.

Note that for both FTP server (119-70) and client (119-3) SMF records, `DSTIP` is on the local z/OS system writing the SMF record, and `SRCIP` is the possibly remote communication partner.

UNIX_ACCESS_INTENT

This field of length 4 is found in RACF processing records (SMF record type 80) , NFS audit statistics records (SMF record type 42 subtype 26), FTP SMF records for actions operating on HFS files (SMF record type 118 subtypes 71, 73, and 74, and SMF record type 119 subtypes 3 and 70), and `ACF2 OMVS CHECK_ACCESS` records. For RACF, it corresponds with the bits in RACF_SECTION(267), "Requested access". For ACF2, it corresponds with the bits in SMFRQACC.

The first character of the field can be:

d Directory search access intended.

- No directory search access intended; this is usually the character for DIRSRCH events

The second character can be:

r Read access intended

- No read access intended

The third character can be:

w Write access intended

- No write access intended

The fourth character can be:

x Execute access intended

- No execute access intended

Select/Exclude syntax for the UNIX_ACCESS_INTENT field is like the NEWLIST TYPE=UNIX field EXTATTR syntax, with characters "drwx" replacing "apsl". For example, you can select on the presence of the "r" and "w" bits with UNIX_ACCESS_INTENT='+rw'M. For information about the (extended) EXTATTR syntax supported for SELECT/EXCLUDE processing, see UNIX formats: Formatting UNIX file type, attribute, and audit flag fields.

USER, USERID

SAF userid. This field is found in the following record types:

- DFSORT records (SMF record type 16)
- Job Initiation and Accounting records (SMF record types 20, 30 and 32)
- RACF processing and R_auditx records (SMF record types 80 and 83)
- NFS audit statistics records (SMF record type 42 subtype 26)
- z/OS Firewall Technologies records (SMF record type 109)
- CICS records (SMF record type 110)

  For CICS subrecords, USER returns the RACF userid that performed the CICS transaction.
- ACF2 records (all subtypes except ACF2 event)
- HSM function statistics records
- DB2® records (SMF record type 102) with subtypes/IFCids 83, 87, 140, 142, 269, and 314 if nonblank and nonnull.
- SMF record type 119 subtypes for sockets (1, 2, and 10), configuration (4), CSSMTP client (48, 50, and 51) FTP client (3), FTP server (70, 72), statistics (6, 7, 8), tunnels (73-80) if non-blank and not null.
- SMF record type 118 subtypes 1, 2 3, 70, 72, 73, 74, 75, 76.

It is derived using the job tag system for data set and ICF catalog activity records (SMF record types 14, 15, 17, 18, 60, 61, 62, 64, 65 and 66).

Note: Some HSM function statistics records may contain the user id **HSM*** or *H*S*M* (the second pseudo-userid starts with a leading zero). These are not SAF userids, but pseudo-userids generated by the HSM software.

To select a userid that is the target of a RACF command, use one of the RACFCMD_USER, RESOURCE or PROFILE fields instead. To select a userid that is the target of an ACF2 command, use ACF2_RULEKEY instead. The USER field describes the command-issuing user, not the target user.

USER_GROUPS

This repeating field returns group names for the user ID. For RACF, these are the connect groups for USER. For ACF2, these are the source groups for the LOGONID, as used by the default DB2 signon exit shipped with ACF2. The field returns no more than 4,000 group names. If the number of privileged connect groups exceeds 4,000, they will be the alphabetically first 4,000 connect groups. The field is filled in for any record type that returns a USER that exists in the security database of the system.

Record types vs. field names

The following fields are now present for more SMF record types:

Table 1. Predefined SMF record types: fields available by record types 66-119, HSM Functions, and ACF2

	66	67	68	69	80	83	86	92	102	109	110	118	119	HSM Func Stats	ACF2
APPLDATA													•		
BYTES_IN												•	•		
BYTES_OUT												•	•		
CIPHER													•		
FIPS140													•		

Table 1. Predefined SMF record types: fields available by record types 66-119, HSM Functions, and ACF2 (continued)

FTP_CIPHERSUITE													•		
FTP_FILETYPE												•	•		
INTENT	•				•	•						•	•		
JOBNAME	•	•	•	•	•	•		•			•		•	•	•
PACKETS_IN													•		
PACKETS_OUT													•		
UNIX_ACCESS_INTENT					•							•	•		•

Printed in USA